Government Printing Office
Future Digital System
Identity and Access Management System Capability Questions

October 19, 2006

This document contains the initial set of questions in support of the Future Digital System Identity and Access Management System (IAMS) evaluation process. The IAMS provides the authentication and authorization capabilities to a large mix of application environments within the Future Digital System (FDsys). The IAMS system ideally will offer comprehensive control of users, security roles and policies, access rules, and auditing through a graphical user interface (GUI).

The solution will need to be capable of providing administration of user attributes, credentials and privileges; and real-time enforcement of assigned privileges via a single sign-on to an enterprise of applications on other platforms. The expected FDsys solution will include a primary site containing all the hardware and software needed to operate the FDsys together with a geographically separated site containing a near real time copy of the entire system. The IAMS solution is required to function whether the sites are connected or completely isolated.

Additional information and clarification questions may be provided to IAMS vendors in the future if needed.

1.0 Requirements Compliance

The accompanying spreadsheet contains selected requirements from the FDsys Requirements Document Version 3.0 that pertain to the IAMS. Please evaluate each requirement in the spreadsheet against the capabilities of your offering. Fill in column C with either a 1 (offering meets the requirement) or 0 (offering does not meet the requirement). If you have separately priced components in your product line, then please record in column D the name of the product in your offering that meets the requirement. If you have any questions or comments about a requirement then record them in column E. Please limit questions and comments to technical information and refrain from including marketing statements.

The IAMS requirements cover a broad range of capabilities. It is understood that every requirement may or not be covered by one product. Some custom coding may be necessary to support some capabilities. Our intent is to determine what range of requirements is covered by each IAMS product and its ease of administration and integration. The product that covers the maximum number of requirements may not be the optimal product for FDsys.

Vendors should be prepared to discuss how their products meet requirements they have indicated are covered and be prepared to demonstrate specific

capabilities of their product. Vendors should bring any equipment and/or software required to demonstrate product functionality in these areas. It is asked that vendors bring ONLY software that is currently shipping and that vendors bring no third party software that is not licensed as part of their application.

2.0 Technical Product Questions

Please answer the following questions as **briefly and concisely** as possible. Lists of components and diagrams **are preferred** to lengthy narratives.

(1) Provide a description of the identity management features offered by your product.

(2) Provide a description of the access management features offered by your product.

(3) Provide an architectural diagram and description of your product, including all necessary supporting components.

(4) What constraints does your product offering place on choices for operating system, server type, networking, back-end repository, etc.?

(5) Provide a description of the user interfaces (i.e., administrative, management, system user, etc.) your product offers.

(6) What type of audit mechanisms does your product provide?

(7) What type of authentication approaches/mechanisms does your product support?

(8) Provide a list of the standards that your product complies with.

(9) What type of workflow support does your product provide?

(10) What user account management (e.g., account, authorization/role, and accountability/audit) functions does your product offer "out of the box"?

(11) Provide a description of how your product provisions user access/roles.

(12) Provide a description of the types of reports your product provides.

(13) Provide a description of your support for a virtual directory (e.g., allowing the enterprise to aggregate identity information from multiple sources in a single view).

(14) Provide a description of your how your product integrates with other Identity and Access Management tools (i.e., enterprise single sign-on, strong authentication, etc.).

(15) Does your system integrate with COTS Content Management Systems (CMS) and COTS web portal systems for role based access control?

(16) What built in method(s) does your system provide for user self-enrollment, and how do they work?

(17) Does your system provide any embedded capability for self service password reset, based on email or web technology? If so, how does this work?

3.0 Cost and Support Questions

(1) Provide an itemized list of the components in your offering and a cost per-user pricing, including different license types and additional maintenance costs.

(2) Describe any advantageous licensing arrangements in your offering.